

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
4 août 2005 (04.08.2005)

PCT

(10) Numéro de publication internationale
WO 2005/071963 A1

(51) Classification internationale des brevets⁷ :
H04N 7/167, H04L 9/14

(74) Mandataire : **POULIN, Gérard**; c/o BREVALEX, 3 rue
du Docteur Lancereaux, F-75008 PARIS (FR).

(21) Numéro de la demande internationale :
PCT/FR2003/050207

(81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,
SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) Date de dépôt international :
23 décembre 2003 (23.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(71) Déposant (*pour tous les États désignés sauf US*) : **VIAC-
CESS** [FR/FR]; Les Collines de l'Arche, Tour Opéra C,
F-92057 PARIS LA DEFENSE CEDEX (FR).

(84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,
TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

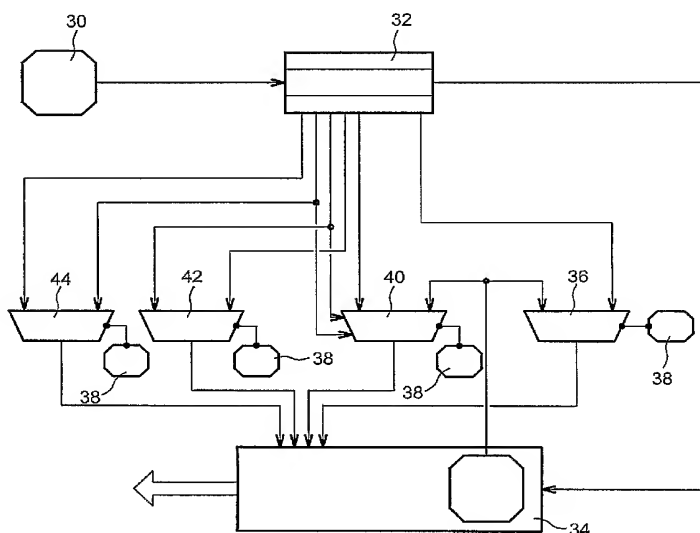
(72) Inventeurs; et

(75) Inventeurs/Déposants (*pour US seulement*) :
DUBROEUCQ, Gilles [FR/FR]; 9 rue Valentin Haüy,
F-75015 PARIS (FR). **VIGARIE, Jean-Pierre** [FR/FR];
32 rue des Tilleuls, F-35510 CESSON SEVIGNE (FR).

[Suite sur la page suivante]

(54) Title: METHOD AND CONDITIONAL ACCESS SYSTEM APPLIED TO THE PROTECTION OF CONTENT

(54) Titre : PROCEDE ET SYSTEME D'ACCES CONDITIONNEL APPLIQUE A LA PROTECTION DE CONTENU



(57) Abstract: The invention relates to a method for controlling access to a transmitted digital data stream which has been previously encrypted. The inventive method comprises the following steps: upon transmission, generation of a message R-ECM_c for controlling the right of access to the recording of the contents of the flow according to a key KR_c, in addition to at least one criterion CRR defining a right to said recording; generation of a message P-ECM_c controlling the right of access to playback of the contents of the flow recorded according to a key KP_c and at least one criterion CRP defining a right to playback, and upon reception, analysis of messages R-ECM_c, and P-ECM_c, and authorization of recording and playback if criteria CRR and CRP are verified.

[Suite sur la page suivante]

WO 2005/071963 A1

**Publiée :**

— avec rapport de recherche internationale

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé. Le procédé selon l'invention comporte les étapes suivantes : à l'émission : générer un message R-ECM_e de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé KR_e, et d'au moins un critère CRR définissant un droit à l'enregistrement, générer un message P-ECM_e de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé KP_e, et d'au moins un critère CRP définissant un droit à la relecture, et à la réception : analyser les messages R-ECM_e, et P-ECM_e, autoriser l'enregistrement et la relecture si les critères CRR et CRP sont vérifiés.

**PROCEDE ET SYSTEME D'ACCES CONDITIONNEL APPLIQUE A LA
PROTECTION DE CONTENU**

DESCRIPTION

5 DOMAINE TECHNIQUE

L'invention se situe dans le domaine du contrôle d'accès et concerne plus particulièrement un procédé et un système d'émission/réception d'informations avec contrôle d'accès à travers un
10 réseau de diffusion MPEG2. Ce procédé est applicable à tout flux de données multiplexé reposant sur l'usage de paquet ou trame.

L'invention concerne également une plate-
forme d'embrouillage et un récepteur de désembrouillage
15 destinés à mettre en œuvre ce procédé.

Plus spécifiquement, l'invention concerne un procédé et un système de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé par une clé de chiffrement CW transmise sous
20 forme chiffrée dans un message de contrôle de titre d'accès ECM (pour "Entitlement Control Message") comportant au moins un critère CA de contrôle d'accès aux données du flux. Les données transmises étant susceptibles d'être déchiffrées à la volée ou
25 enregistrées telles quelles dans un terminal récepteur.

ETAT DE LA TECHNIQUE ANTERIEURE

Afin de lutter contre le piratage de données et de services distribués en ligne, notamment
30 via le réseau Internet, il devient primordial pour les

opérateurs de protéger ces données en phase de diffusion et après la diffusion.

La figure 1 représente un schéma général d'un système de contrôle d'accès de l'art antérieur
5 dans lequel une plate-forme d'embrouillage 2, agencée généralement en tête de réseau, reçoit un flux en clair F_x et fournit à un terminal récepteur 4 un contenu chiffré F_{xs} . La plate-forme 2 comporte un générateur 6 de clés CW_i d'embrouillage et de désembrouillage, un
10 générateur messages de contrôle de titre d'accès (ECM) 8, et un générateur messages de gestion de titre d'accès (EMM) (pour "Entitlement Management Message") 10. Le terminal récepteur 4 comporte un module de désembrouillage 12, un processeur de sécurité 14
15 comportant un module de déchiffrement 16 des clés de contrôle CW_i et une mémoire 18.

Avant la diffusion des flux de données, ceux-ci sont embrouillés par la plate-forme d'embrouillage 2 au moyen des clés CW_i . Afin de
20 permettre le désembrouillage du contenu des flux diffusés, les clés de désembrouillage CW_i sont transmises aux terminaux 4 sous forme chiffrée dans les messages de contrôle de titre d'accès ECM avec au moins un critère CA de contrôle d'accès. Après vérification
25 des critères d'accès au moyen d'un comparateur 20 à des droits préalablement transmis aux terminaux 4, dans les messages de gestion de titre d'accès (EMM) et inscrits dans la mémoire 18, les clés de désembrouillage CW_i sont déchiffrées puis transmises au module de
30 désembrouillage 12.

Pour améliorer la sécurité globale du système, les clés de désembrouillage CW_i changent régulièrement sur des crypto-périodes CP_i (typiquement quelques secondes) et sont généralement appliquées au désembrouilleur 12 par couple $[CW_i, CW_{i+1}]$ où CW_i représentant la clé de désembrouillage valable pendant la crypto-période CP_i , et CW_{i+1} représentant la clé de désembrouillage valable pendant la crypto-période CP_{i+1} . Chaque clé de désembrouillage à utiliser est référencée par un bit indiquant la parité de i de sorte qu'à chaque changement d'ECM, deux clés de désembrouillage, une paire ECW et une impaire OCW, sont configurées sur le désembrouilleur avant le changement effectif de crypto-période.

15 Dans un contexte de télédiffusion, une technique connue pour protéger le contenu une fois diffusé consiste à enregistrer ce contenu avec la signalisation d'accès conditionnel associée.

Un premier inconvénient de cette solution provient du fait qu'elle ne permet pas d'associer des critères d'accès distincts pour les phases :

- de visualisation directe du contenu depuis le flux ;
- d'enregistrement du contenu ; et
- 25 - de visualisation du flux depuis le contenu enregistré localement.

Un second inconvénient de cette technique provient du fait que les clés secrètes d'exploitation stockées dans un processeur de sécurité et servant au déchiffrement des ECMs sont régulièrement mises à jour. Dans ce cas, les ECM stockés avec le contenu ne sont

plus valides et ce dernier devient inexploitable même si le client a acquis des droits d'utilisation dépassant cette période.

Un troisième inconvénient est lié aux aspects de synchronisation entre la fourniture et l'exploitation des clés de désembrouillage CW_i lors d'une exploitation d'un contenu enregistré. Dans ce cas, la fonction de lecture arrière ne peut pas être réalisée de manière simple, car la valeur anticipée de la prochaine clé de désembrouillage (représentant la clé de désembrouillage précédente) n'est pas fournie dans l'ECM.

Une autre technique connue dans l'art antérieur pour protéger le contenu est l'utilisation d'une solution dite DRM (pour Digital Right Management).

Ce type de solution repose sur :

- l'usage de certificats pour établir une chaîne de confiance entre les composants du système ;
- un chiffrement ou pré-embrouillage du contenu à l'aide d'un algorithme à clé privé ;
- l'envoi en ligne de cette clé privée associée aux droits d'utilisations pour former une licence chiffrée à l'aide d'un algorithme de chiffrement utilisant une clé publique du client.

Cette solution n'est pas adaptée au contexte de la télédiffusion dans lequel l'usage d'une voie de retour n'est pas systématique. De plus, ce type de solution ne permet pas de conditionner l'accès au contenu moyennant la possession de droits inscrits

indifféremment par voie hertzienne ou en ligne dans un processeur de sécurité.

Le but de l'invention est de pallier les inconvénients de l'art antérieur décrits ci-dessus au moyen d'un procédé et d'un dispositif utilisant un processus d'embrouillage basé sur des changements périodiques de mots de contrôle et assurant une compatibilité ascendante avec les systèmes d'accès conditionnel antérieurs.

10

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé au moyen d'une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM comportant en outre au moins un critère CA de contrôle d'accès, lesdites données numériques étant susceptibles d'être enregistrées telles quelles dans un terminal récepteur ou déchiffrées à la volée.

20

Selon l'invention, ce procédé comporte les étapes suivantes :

à l'émission :

- générer un message R-ECM_c de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé d'enregistrement KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message P-ECM_c de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé de relecture KP_c et d'au moins

30

un critère CRP définissant un droit à la relecture,
et

à la réception :

- analyser le message R-ECM_c, et
- 5 - autoriser l'enregistrement si le critère CRR est vérifié, sinon, interdire l'enregistrement,
- analyser le message P-ECM_c, et
- autoriser la relecture si le critère CRP est vérifié, sinon, interdire la relecture.

10

Selon une première variante de réalisation du procédé de l'invention, les clés CW, KR_c et KP_c sont chiffrées par une première clé de service K_s.

15

Selon une deuxième variante de réalisation du procédé de l'invention les clés CW, KR_c et KP_c sont chiffrées par trois clés de service différentes respectivement K_s, K_{SR} et K_{SP}.

20

Dans un premier mode de réalisation, la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une
- 25 durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,
- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,
- 30 - calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés de chiffrement

CW_{i-1} , CW_i , CW_{i+1} préalablement définies, de la valeur $p(i)$ et du critère CA_i , ledit message SC-ECM_i étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1} , CW_i , CW_{i+1} au moyen de la clé de relecture KP_c ,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s ,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c .

Dans un deuxième mode de réalisation, la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données :

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i , et, à chaque changement de crypto-période i ,

- embrouiller le contenu du flux au moyen de la clé CW_i , et mémoriser une valeur $p(i)$ représentative de la parité de i ,

- calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés de chiffrement CW_{i-1} , CW_i , CW_{i+1} préalablement définies, de la valeur $p(i)$ et du critère CA_i , ledit message SC-ECM_i étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une deuxième clé de service K'_s ,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé de relecture KP_c ,

5 - chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c .

10 Dans les deux modes de réalisation, la phase de l'émission comporte en outre les étapes consistant :

- calculer le message de contrôle de titre d'accès $ECM_i = f[(ECW_i, OCW_i, CA)]$ où, ECW_i et OCW_i représentent respectivement les mots de contrôle pair et impair préalablement chiffrés au moyen d'une première clé de service K_s ,

$ECW_i = CW_i$ si i pair sinon $ECW_i = CW_{i+1}$;

$OCW_i = CW_i$ si i impair sinon $OCW_i = CW_{i+1}$;

20 - diffuser dans la signalisation ECM des paramètres identifiant les voies ECM rattachées au service diffusant le contenu des messages ECM_i , $P-ECM_c$, $R-ECM_c$, $SC-ECM_i$,

- fournir au terminal récepteur les messages ECM_i , $P-ECM_c$, $R-ECM_c$, $SC-ECM_i$

25

Deux modes de distribution des messages ECM_i , $P-ECM_c$, $R-ECM_c$, $SC-ECM_i$ sont possibles. Ces derniers peuvent être soit diffusés sur la voie ECM associée au contenu du segment S_i , soit délivrés en partie au terminal récepteur à partir d'un Serveur

30

d'Autorisation en tête de réseau sur requête et en fonction du type d'exploitation du contenu envisagé.

Ainsi, les message R-ECM et/ou P-ECM peuvent être délivrés au terminal récepteur sur requête
5 à partir d'un Serveur d'Autorisation en tête de réseau si l'enregistrement et/ou la relecture sont envisagés.

Selon l'invention, pour recevoir directement le flux reçu, la phase de la réception comporte les étapes suivantes :

10 - récupérer la voie ECM du message ECM_i à partir de la signalisation rattachée au service diffusant le flux de données, et à chaque changement de i ,

- analyser le message ECM_i afin de récupérer
15 les mots de contrôle pair OCW, et impair ECW, pour désembrouiller le contenu du flux diffusé de manière à obtenir un accès direct à ce contenu.

Pour enregistrer le flux reçu, la phase de la réception comporte les étapes suivantes :

20 - récupérer la voie ECM des messages P- ECM_c , R- ECM_c , SC- ECM_i à partir de la signalisation rattachée au service diffusant le contenu ;

- analyser le message R- ECM_c pour vérifier les critères d'accès à l'enregistrement CRR

25 - mémoriser la clé d'enregistrement KR_c ;
- récupérer le message P- ECM_c et le stocker avec le contenu ; et

pour chaque crypto-période i :

- récupérer le message SC- ECM_i ,
30 - déchiffrer le message SC- ECM_i au moyen de la clé d'enregistrement KR_c , et

- enregistrer le message SC-ECM_i déchiffré avec le contenu.

Selon l'invention, l'accès à la relecture du contenu du flux enregistré est obtenu selon les
5 étapes suivantes :

- récupérer le message P-ECM_c dans le contenu et l'analyser pour vérifier les critères d'accès à la lecture CRP,
- mémoriser la clé de relecture KP_c ; et
- 10 - récupérer dans le contenu le message SC-ECM_i courant ;
- déchiffrer le message SC-ECM_i avec la clé de relecture KP_c et vérifier les critères d'accès,
- récupérer les clés chiffrées CW_{i-1}, CW_i,
15 CW_{i+1} et la valeur p(i) indiquant la parité de i, et
- déchiffrer, au moyen de la deuxième clé K'_s, lesdites clés suivant le sens de lecture pour en déduire ECW et OCW ; puis,
- appliquer soit ECW, soit OCW pour
20 désembrouiller le contenu à la relecture.

Dans une autre variante, l'accès à la relecture du contenu du flux est obtenu selon les étapes suivantes :

- 25 - récupérer le message P-ECM_c dans le contenu,
- analyser le message P-ECM_c pour vérifier les critères d'accès à la lecture CRP,
- mémoriser KP_c, et
- 30 - récupérer dans le contenu le message SC-ECM_i courant,

- déchiffrer le message SC-ECM_i avec la deuxième clé de service K's et vérifier les critères d'accès,

- 5 - récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et
- déchiffrer, au moyen de la deuxième clé KRc lesdites clés suivant le sens de lecture pour en déduire ECW et OCW ; puis,
- 10 - appliquer soit ECW, soit OCW pour désembrouiller le contenu.

Préférentiellement, la phase de réception comporte en outre les étapes suivantes :

- 15 - générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,
- sur-chiffrer localement le contenu à enregistrer par cette clé K_I.
- 20 - à la relecture, régénérer la clé K_I à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,
- déchiffrer le contenu enregistré au moyen
- 25 de la clé K_I régénérée.

Dans une application particulière du procédé selon l'invention, les données numériques diffusées représentent des programmes audiovisuels.

L'invention concerne également un système de contrôle d'accès à un flux de données numériques comportant une plate-forme d'embrouillage comprenant au moins un générateur de messages de contrôle de titre d'accès ECM et au moins un récepteur de désembrouillage muni d'un processeur de sécurité.

Selon l'invention, la plate-forme d'embrouillage comporte en outre:

- un générateur de messages R-ECM_c de contrôle de titre d'accès à l'enregistrement du contenu du flux reçu et un générateur de messages P-ECM_c de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré, et le récepteur de désembrouillage comporte :
- des moyens pour récupérer la voie ECM des messages P-ECM_c, R-ECM_c,
- des moyens pour déchiffrer le contenu d'un flux reçu pour l'enregistrer,
- des moyens pour déchiffrer le contenu d'un flux enregistré pour le relire.

Préférentiellement, le récepteur de désembrouillage comporte en outre des moyens pour générer une clé locale K_r à partir d'attributs contenus dans le message R-ECM et de l'identité du terminal-récepteur pour chiffrer/déchiffrer localement le contenu du flux reçu.

L'invention concerne également une plate-forme d'embrouillage comportant au moins un générateur de messages de contrôle de titre d'accès ECM à un flux de donnée diffusé sous forme embrouillée, un générateur de messages R-ECM_c de contrôle de titre d'accès à

l'enregistrement du contenu d'un flux reçu et un générateur de messages P-ECM_c de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré.

La plate-forme d'embrouillage comporte en outre :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i,
- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW_i,
- des moyens pour calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés CW_{i-1}, CW_i, CW_{i+1} correspondant respectivement aux crypto-périodes CP_i, CP_{i-1} et CP_{i+1}, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA_i, ledit message SC-ECM_i étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,
- des moyens pour chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une clé de relecture KP_c,
- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,
- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

L'invention concerne également un récepteur de désembrouillage d'un flux de donné diffusé sous forme embrouillée par une clé d'embrouillage CW_i

comportant un processeur de sécurité dans lequel est mémorisée au moins une clé d'enregistrement KR_c destinée à désembrouiller des messages de contrôle d'accès à l'enregistrement $R-ECM_c$ et au moins une clé
5 de relecture KP_c destinée à désembrouiller des messages de contrôle d'accès à la relecture $P-ECM_c$,

Selon l'invention, ce récepteur comporte :

- des moyens pour récupérer la voie ECM des messages $P-ECM_c$, et des messages $R-ECM_c$ à partir de la
10 signalisation rattachée au service diffusant le contenu ;

- des moyens pour déchiffrer le message $R-ECM_c$ au moyen de la clé d'enregistrement KR_c pour vérifier le droit à enregistrer le contenu d'un flux
15 reçu,

- des moyens pour déchiffrer le message $P-ECM_c$ au moyen de la clé de relecture KP_c pour vérifier le droit à relire le contenu d'un flux enregistré,

Préférentiellement, le récepteur selon
20 l'invention comporte en outre des moyens pour générer une clé K_I à partir de l'identité du récepteur pour chiffrer et déchiffrer localement le contenu du flux reçu.

Dans un mode de réalisation préféré de
25 l'invention, le processeur de sécurité est une carte à puce.

BREVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de
30 l'invention ressortiront de la description qui va

suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées dans lesquelles :

- la figure 1, décrite précédemment, représente un schéma général d'un système de contrôle d'accès de l'art antérieur ;
- la figure 2 représente un schéma bloc illustrant la phase d'embrouillage des flux à diffuser par un système de contrôle d'accès selon l'invention,
- la figure 3 illustre schématiquement le processus de contrôle d'accès à l'enregistrement d'un flux de données selon l'invention,
- la figure 4 illustre schématiquement le processus de contrôle d'accès à la relecture du flux de données enregistré selon l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

La description qui suit sera faite dans le cadre d'une application particulière dans laquelle les flux diffusés représentent des programmes audiovisuels nécessitant un droit d'accès.

Dans cette application, le procédé repose sur une diffusion de contenu à travers une structure de paquets multiplexés dont la forme est indiquée à l'annexe 1.

La signalisation du programme diffusant le contenu comprend une description précise indiquant les voies du multiplex par un identifiant de paquet « Packet Identifier » en anglais utiles à la réception du contenu ainsi que la nature des données transmises dans chaque voie (composante son, vidéo ou autre).

Cette signalisation comprend un descripteur d'accès conditionnel "CA_descriptor" indiquant la présence et la localisation des voies transportant les ECMs. Ce descripteur est associé soit au niveau global du programme, soit au niveau de chaque déclaration d'une voie composante.

Le format de ce descripteur est standard dans le cas d'une diffusion MPEG2 ISO13818-1 représenté à l'annexe 2.

Les données privées "private_data_byte" pour le procédé décrit sont décrites dans l'annexe 3 pour un mode de réalisation.

Elles ont un suffixe XID dans l'entête des ECMs et servent de discriminant pour distinguer les ECM véhiculés éventuellement sur la même voie paquet.

Lorsqu'une partie des voies ECM_i , $P-ECM_c$, $R-ECM_c$, $SC-ECM_i$ est absente, les combinaisons possibles sont les suivantes .;

- voie ECM_i absente : pas de visualisation immédiate ;
- voie $R-ECM_c$ absente : enregistrement interdit ou si le terminal récepteur dispose d'une voie de retour opérationnelle, se connecter à un Serveur d'Autorisation en tête de réseau délivrant le message $R-ECM_c$ nécessaire à l'enregistrement du contenu ;
- voie $P-ECM_c$ absente : lecture interdite ou si le terminal récepteur dispose d'une voie de retour opérationnelle, se connecter à un Serveur d'Autorisation en tête de réseau délivrant le message $P-ECM_c$ nécessaire à la lecture du contenu enregistré;
- voie $SC-ECM_i$ absente : alors $R-ECM_i$ et $P-ECM_i$ sont absentes et l'enregistrement n'est pas autorisé.

Selon la nature des données transmises, signalisation ou composante audio ou son, la charge utile « payload » en anglais est chiffrée ou non par la plate-forme d'embrouillage 2 et la valeur du champ "Scrambling Control" prend les valeurs suivantes :

- le paquet n'est pas embrouillé,
- le paquet est embrouillé par le mot de contrôle pair ECW,
- le paquet est embrouillé par le mot de contrôle impair OCW.

La figure 2 illustre schématiquement la phase d'embrouillage des flux à diffuser par un système de contrôle d'accès selon l'invention.

L'étape 30 consiste à générer une clé secrète d'enregistrement KR_c de contrôle d'accès à l'enregistrement et une clé secrète de relecture KP_c de contrôle d'accès à la relecture.

L'étape 32 consiste à découper, pour chaque flux de données, la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i . Les paquets ainsi constitués sont ensuite appliqués à un module d'embrouillage et de multiplexage 34 qui reçoit parallèlement un message ECM_i contenant les clés de désembrouillage CW_i , CW_{i+1} de contrôle de titre d'accès au contenu du flux et au moins un critère d'accès CA_i , un message $SC-ECM_i$ contenant les clés de désembrouillage CW_{i-1} , CW_i , CW_{i+1} de contrôle de titre d'accès au contenu d'un segment S_i de données correspondant à au moins deux crypto-périodes, un

message R-ECM_c contenant la clé d'enregistrement KR_c de
contrôle d'accès à l'enregistrement du contenu du
segment S_i et au moins un critère CRR définissant un
droit à l'enregistrement de ce contenu, et un message
5 P-ECM_c contenant la clé de relecture KP_c de contrôle
d'accès à la relecture du contenu du segment S_i
enregistré et au moins un critère CRP de contrôle
d'accès à la relecture du contenu de ce segment.

Préalablement, à l'étape 36, les clés de
10 désembrouillage CW_i, CW_{i+1} sont chiffrées par une
première clé secrète de service K_s extraite d'une carte
à puce 38, et à l'étape 40, les clés de désembrouillage
CW_{i-1}, CW_i, CW_{i+1} sont chiffrées successivement par la clé
d'enregistrement KR_c puis par la clé de relecture KP_c, à
15 l'étape 42, la clé KP_c est chiffrée par une deuxième
clé de service K'_s extraite de la carte à puce 38, et à
l'étape 44, la clé KR_c est chiffrée par la deuxième clé
de service K'_s.

Les messages ECM_i, R-ECM_i, P-ECM_i et SC-ECM_i
20 à diffuser sont ensuite appliqués au module
d'embrouillage et de multiplexage 34 pour être
multiplexés avec le paquet de données et transmis au
terminal récepteur.

Notons que l'étape 42 revient à réaliser un
25 sur-chiffage des mots de contrôle CW_{i-1}, CW_i, CW_{i+1}
successivement au moyen de la clé de relecture KP_c, de
la deuxième clé de service K'_s, puis de la clé
d'enregistrement KR_c.

Dans une variante de réalisation ce sur-
30 chiffage des mots de contrôle CW_{i-1}, CW_i, CW_{i+1} est

réalisé successivement au moyen de la clé K'_s , au moyen de la clé de relecture KP_c , puis au moyen de la clé KR_c .

La figure 3 illustre schématiquement la phase de réception et de désembrouillage d'un contenu diffusé en vue de son enregistrement.

L'étape 50 consiste à rechercher les voies ECM présentes des messages $P-ECM_c$, $R-ECM_c$, $SC-ECM_i$ dans la signalisation rattachée au service diffusant le contenu.

L'étape 51 n'est réalisée que si le message $R-ECM_c$ est absent de la diffusion. Une condition supplémentaire est que le terminal récepteur dispose d'un dispositif de commutation bidirectionnelle. L'étape 51 consiste à se connecter à un Serveur d'Autorisation en déclinant l'identifiant du contenu à enregistrer et l'identité du terminal client. Selon des critères connus du Serveur d'Autorisation, ce dernier délivre en ligne le $R-ECM_c$ nécessaire à l'enregistrement du contenu.

A l'étape 52, le message $R-ECM_c$ est présenté au processeur de sécurité qui après vérification des critères d'accès à l'enregistrement mémorise la clé KR_c . L'étape 52 n'est réalisée qu'à condition d'une diffusion du message $P-ECM_c$.

A l'étape 54, le message $P-ECM_c$ est récupéré puis stocké en l'état dans l'entête du fichier de stockage du contenu.

A l'étape 56, pour chaque crypto-période i , le message $SC-ECM_i$ est récupéré puis présenté au processeur de sécurité qui le déchiffre avec la clé KR_c pour récupérer un message déchiffré $SC-ECM_i$ qui est

ensuite enregistré avec les paquets du multiplex constituant le contenu.

Dans une variante de réalisation, ces paquets du multiplex sont chiffrés localement (étape 5 58) avec une clé K_I générée à l'étape 60 à partir d'attributs contenus dans le message $K-EMC_c$ et d'un paramètre relatif à l'identité du décodeur. A titre d'exemple, ce paramètre peut être le numéro de série du décodeur, l'identifiant unique (UA) de la carte à puce 10 ou encore le numéro de série d'un disque dur équipant le terminal récepteur.

La figure 4 illustre schématiquement la phase de désembrouillage d'un contenu enregistré dans un support d'enregistrement 60 en vue de sa relecture.

15 L'étape 62 consiste à rechercher le message $P-ECM_c$ dans l'entête du fichier contenant les données du flux.

L'étape 63 suivante n'est réalisée que si le message $P-ECM_c$ est absent de l'entête du fichier 20 contenant. Une condition supplémentaire est que le terminal dispose d'un dispositif de communication bidirectionnelle. L'étape 63 consiste à se connecter à un Serveur d'Autorisation en déclinant l'identifiant du contenu à lire et l'identité du terminal client. Selon 25 des critères connus du Serveur d'Autorisation, ce dernier délivre en ligne $P-ECM_c$ nécessaire à la lecture du contenu.

A l'étape 64, le message $P-ECM_c$ retrouvé est présenté au processeur de sécurité qui après 30 vérification des critères d'accès à la lecture mémorise la clé de relecture KP_c dans la carte à puce 38.

Si le contenu a été préalablement embrouillé localement conformément à l'étape 58 décrite précédemment, la clé locale d'identité K_I est alors calculée à partir des informations d'identité du terminal récepteur (étape 68), et pour chaque crypto-période i , le multiplex du contenu est déchiffré à la lecture à la volée avec la clé K_I (étape 70).

Dans un mode préféré de réalisation de l'invention, à la relecture, la clé K_I est régénérée à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur et est utilisée pour déchiffrer le contenu enregistré.

À l'étape 72, le message SC-ECM _{i} courant est récupéré, puis présenté au processeur de sécurité (étape 74) qui le déchiffre avec la clé K_P pour vérifier les critères d'accès CRP à la relecture et récupérer les mots de contrôle CW_{i-1} , CW_i , CW_{i+1} et la parité de i . Suivant le sens de lecture souhaité, une des clés de désembrouillage ECW ou OCW est fournie au désembrouilleur pour désembrouiller le segment de données S_i .

Dans le cas où le segment S_i doit être visualisé directement, le procédé selon l'invention permet de rechercher la voie ECM et l'indexe des ECM _{i} dans la signalisation rattachée au service diffusant le contenu à chaque changement de i et d'appliquer l'ECM _{i} au processeur de sécurité pour récupérer les mots de contrôle pair et impair OCW, ECW et les appliquer au désembrouilleur 80.

ANNEXE 1

Packet IDentifier	Scrambling Control	Payload : Data bytes + padding bytes
----------------------	-----------------------	-----------------------------------------

Une définition équivalente est

```
5  CAS_PACKET_UNIT()  
   {  
       Packet IDentifier          x bits ;  
       Scrambling_Control         2 bits ;  
       Payload  z bytes  
10  }  
   x+2 multiple de 8 ;  
   La séquence payload se décompose en Payload()  
   {  
       data bytes                  m octets  
15  padding bytes                  p octets  
                                     }  
   }
```


ANNEXE 2

```
5  CA_descriptor()  
   {  
       descriptor_tag = 0x09           8 bits  
       descriptor_length           8 bits  
       CA_system_ID               16 bits  
       reserved                   3 bits  
10      CA_PID                   13 bits  
       for (i=0; i<N; i++) {  
           private_data_byte       8 bits
```

ANNEXE 3

```

private data bytes ()
{
5   Si Voie ECM présente dans le multiplex (voir) :
   {
       ECM_CHANNEL_TAG                1 octet
indicateur de descripteur voie SC_ECM
       ECM_XID ;                      1 octet
10  indice de l'ECM Stream dans la voie paquet
       ECM_CI ;                      1 octet
version du crypto-algorithme pour l'ECM Stream
       ECM_SOID ;                    3 octets
référence du jeu de clé privé utilisé pour le Stream
15 }

   Si Voie SC_ECM présente dans le multiplex :
   ( // Extension du système
       SC_ECM_CHANNEL_TAG            1 octet
indicateur de descripteur voie SC_ECM
20  PPS_ECM_CI;                      1 octet
Version du crypto-algorithme pour les ECM "contenus"
       SC_ECM_SOID;                  3 octets
SOID des SC_ECM
       SC_ECM_PID ;                  x octets
25  identité de la voie paquet pour les SC_ECM
       SC_ECM_XID ;                  1 octet
indice du SC_ECM dans la voie paquet

       Si Voie R_ECM présente dans le multiplex :
30  {
       R_ECM_CHANNEL_TAG            1 octet
indicateur de descripteur voie R_ECM
       R_ECM_SOID;                  3 octets
SOID des R_ECM
35  R_ECM_PID ;                      x octets
identité de la voie paquet pour les R_ECM
       R_ECM_XID;                    1 octet
indice du R_ECM dans la voie paquet
   }
40

   Si Voie P_ECM présente dans le multiplex :
   {
       P_ECM_CHANNEL_TAG            1 octet
indicateur de descripteur voie P_ECM

```

25

```
        P_ECM_SOID;                                3 octets
SOID des P_ECM
        P_ECM_PID ;                                x octets
identité de la voie paquet pour les R_ECM
5      P_ECM_XID;                                1 octet
indexe du P_ECM dans la voie paquet
    }
```

10

REVENDEICATIONS

1. Procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé
5 au moyen d'une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM comportant en outre au moins un critère CA de contrôle d'accès, lesdites données numériques étant susceptibles d'être enregistrées telles quelles dans un
10 terminal récepteur ou déchiffrées à la volée, procédé caractérisé en ce qu'il comporte les étapes suivantes :

à l'émission :

- générer un message R-ECM_c de contrôle de titre d'accès à l'enregistrement du contenu du flux en
15 fonction d'une clé d'enregistrement KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message P-ECM_c de contrôle de titre d'accès à la relecture du contenu du flux enregistré
20 en fonction d'une clé de relecture KP_c et d'au moins un critère CRP définissant un droit à la relecture, et

à la réception :

- analyser le message R-ECM_c, et
- 25 - autoriser l'enregistrement si le critère CRR est vérifié, sinon, interdire l'enregistrement,
- analyser le message P-ECM_c, et
- autoriser la relecture si le critère CRP est vérifié, sinon, interdire la relecture.

2. Procédé selon la revendication 1, caractérisé en ce que les clés CW , KR_c et KP_c sont chiffrées par une première clé de service K_s .

5 3. Procédé selon la revendication 1, caractérisé en ce que les clés CW , KR_c et KP_c sont chiffrées par trois clés de service différentes respectivement K_s , K_{SR} et K_{SP} .

10 4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données

15 - découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i , et à chaque changement de crypto-période,

20 - embrouiller le contenu du flux au moyen de la clé CW_i , et mémoriser une valeur $p(i)$ représentative de la parité de i ,

25 - calculer un message de contrôle de titre d'accès $SC-ECM_i$ en fonction des clés de chiffrement CW_{i-1} , CW_i , CW_{i+1} préalablement définies, de la valeur $p(i)$ et du critère CA_i , ledit message $SC-ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1} , CW_i , CW_{i+1} au moyen de la clé de relecture KP_c ,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s ,

5 - chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c .

5. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la phase de l'émission
10 comporte les étapes suivantes :

 pour chaque flux de données :

 - découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i , et à
15 chaque changement de crypto-période,

 - embrouiller le contenu du flux au moyen de la clé CW_i , et mémoriser une valeur $p(i)$ représentative de la parité de i ,

 - calculer un message de contrôle de titre
20 d'accès $SC-ECM_i$ en fonction des clés de chiffrement CW_{i-1} , CW_i , CW_{i+1} préalablement définies, de la valeur $p(i)$ et du critère CA_i , ledit message $SC-ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-
25 périodes,

 - chiffrer les clés CW_{i-1} , CW_i , CW_{i+1} au moyen d'une deuxième clé de service K'_s ,

 - chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé KP_c ,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c .

5 6. Procédé selon les revendications 4 ou 5, caractérisé en ce que la phase de l'émission comporte en outre les étapes consistant :

 - calculer le message de contrôle de titre d'accès $ECM_i = f[(ECW_i, OCW_i, CA)]$ où, ECW_i et OCW_i
10 représentent respectivement les mots de contrôle pair et impair préalablement chiffrés au moyen d'une première clé de service K_s ,

$ECW_i = CW_i$ si i pair sinon $ECW_i = CW_{i+1}$;

$OCW_i = CW_i$ si i impair sinon $OCW_i = CW_{i+1}$;

15 - diffuser dans la signalisation ECM des paramètres identifiant les voies ECM rattachées au service diffusant le contenu des messages ECM_i , P- ECM_c , R- ECM_c , SC- ECM_i ,

 - fournir au terminal récepteur les
20 messages ECM_i , P- ECM_c , R- ECM_c , SC- ECM_i .

 7. Procédé selon la revendication 6, caractérisé en ce que les messages ECM_i , P- ECM_c , R- ECM_c , SC- ECM_i sont diffusés par voies ECM associées au contenu
25 du segment S_i .

 8. Procédé selon la revendication 6, caractérisé en ce que, le message R-ECM est délivré au terminal récepteur sur requête à partir d'un Serveur
30 d'Autorisation en tête de réseau.

9. Procédé selon la revendication 6, caractérisé en ce que, le message P-ECM est délivré au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau.

5

10. Procédé selon la revendication 7, caractérisé en ce que la phase de la réception comporte les étapes suivantes :

10 - récupérer la voie ECM du message ECM_i à partir de la signalisation rattachée au service diffusant le flux de données, et à chaque changement de i ,

15 - analyser le message ECM_i afin de récupérer les mots de contrôle pair OCW, et impair ECW, pour désembrouiller le contenu du flux diffusé de manière à obtenir un accès direct à ce contenu.

11. Procédé selon la revendication 7, caractérisé en ce que la phase de la réception comporte les étapes suivantes :

20 - récupérer la voie ECM des messages P- ECM_c , R- ECM_c , SC- ECM_i à partir de la signalisation rattachée au service diffusant le contenu ;

25 - analyser le message R- ECM_c pour vérifier les critères d'accès à l'enregistrement CRR,

- mémoriser la clé d'enregistrement KR_c ;

- récupérer le message P- ECM_c et le stocker avec le contenu ; et

pour chaque crypto-période i :

30 - récupérer le message SC- ECM_i ,

- déchiffrer le message SC-ECM_i au moyen de la clé d'enregistrement KR_c, et

- enregistrer le message SC-ECM_i déchiffré avec le contenu.

5

12. Procédé selon la revendication 7, caractérisé en ce que l'accès à la relecture du contenu du flux enregistré est obtenu selon les étapes suivantes :

- 10 - récupérer le message P-ECM_c dans le contenu et l'analyser pour vérifier les critères d'accès à la lecture CRP,

- mémoriser la clé de relecture KP_c ; et

- récupérer dans le contenu le message SC-ECM_i courant,

- 15 - déchiffrer le message SC-ECM_i avec la clé de relecture KP_c et vérifier les critères d'accès,

- récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et

- 20 - déchiffrer lesdites clés suivant le sens de lecture pour en déduire ECW et OCW, puis,

- appliquer soit ECW, soit OCW pour désembrouiller le contenu à la relecture.

25 13. Procédé selon la revendication 7, caractérisé en ce que l'accès à la relecture du contenu du flux est obtenu selon les étapes suivantes :

- récupérer le message P-ECM_c dans le contenu,

- 30 - analyser le message P-ECM_c pour vérifier les critères d'accès à la lecture CRP,

- mémoriser KP_c , et
- récupérer dans le contenu le message SC-ECM_i courant ;
- déchiffrer le message SC-ECM_i avec la
5 deuxième clé de service K'_s et vérifier les critères d'accès,
- récupérer les clés chiffrés CW_{i-1} , CW_i , CW_{i+1} et la valeur $p(i)$ indiquant la parité de i , et
- déchiffrer lesdites clés suivant le sens
10 de lecture pour en déduire ECW et OCW, puis,
- appliquer soit ECW, soit OCW pour désembrouiller le contenu.

14. Procédé selon la revendication 11 ou
15 12, caractérisé en ce que la phase de réception comporte en outre les étapes suivantes :

- générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et d'au moins un paramètre relatif à l'identité du terminal-
20 récepteur,
- sur-chiffrer localement le contenu à enregistrer par cette clé K_I , et
- à la relecture, régénérer la clé K_I à partir d'attributs contenus dans le message P-ECM et
25 d'au moins un paramètre relatif à l'identité du terminal-récepteur,
- déchiffrer le contenu enregistré au moyen de la clé K_I régénérée.

15. Procédé selon l'une des revendications 1 à 14, caractérisé en ce que les données numériques diffusées représentent des programmes audiovisuels.

5 16. Système de contrôle d'accès à un flux de données numériques comportant une plate-forme d'embrouillage (2) comprenant au moins un générateur de messages de contrôle de titre d'accès ECM et au moins un récepteur de désembrouillage (4) muni d'un
10 processeur de sécurité (14), caractérisé en ce que la plate-forme d'embrouillage (2) comporte en outre :

 - un générateur de messages R-ECM_c de contrôle de titre d'accès à l'enregistrement du contenu du flux reçu et un générateur de messages P-ECM_c de
15 contrôle de titre d'accès à la relecture du contenu d'un flux enregistré, et en ce que le récepteur de désembrouillage (4) comporte :

 - des moyens pour récupérer la voie ECM des messages P-ECM_c, R-ECM_c,
20 - des moyens pour déchiffrer le contenu d'un flux reçu pour l'enregistrer, et
 - des moyens pour déchiffrer le contenu d'un flux enregistré pour le relire.

25 17. Système selon la revendication 16, caractérisé en ce que le récepteur de désembrouillage (4) comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM_c et de l'identité du terminal-récepteur pour
30 chiffrer/déchiffrer localement le contenu du flux reçu.

18. Plate-forme d'embrouillage (2)
comportant au moins un générateur de messages de
contrôle de titre d'accès ECM à un flux de donnée
diffusé sous forme embrouillée, caractérisée en ce
5 qu'elle comporte en outre un générateur de messages
R-ECM_c de contrôle de titre d'accès à l'enregistrement
du contenu d'un flux reçu et un générateur de messages
P-ECM_c de contrôle de titre d'accès à la relecture du
contenu d'un flux enregistré.
- 10
19. Plate-forme d'embrouillage selon la
revendication 18, caractérisée en ce qu'elle comporte :
- des moyens pour découper la période
d'embrouillage en une suite de crypto-périodes CP_i
15 définissant chacune une durée de validité d'une clé
individuelle CW_i ,
 - des moyens pour chiffrer le contenu du
flux à chaque changement de crypto-période i au moyen
de la clé CW_i ,
 - 20 - des moyens pour calculer un message de
contrôle de titre d'accès SC-ECM_i en fonction des clés
 CW_{i-1} , CW_i , CW_{i+1} correspondant respectivement aux
crypto-périodes CP_i , CP_{i-1} et CP_{i+1} , d'un paramètre de
parité $p(i)$ et du critère de contrôle d'accès CA_i ,
25 ledit message SC-ECM_i étant destiné à véhiculer des
droits d'accès à un segment S_i de données correspondant
à au moins deux crypto-périodes,
 - des moyens pour chiffrer les clés CW_{i-1} ,
 CW_i , CW_{i+1} au moyen d'une clé de relecture KP_c ,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s ,

- des moyens pour chiffrer le résultat du
5 chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c .

20. plate-forme selon la revendication 18, caractérisé en ce qu'elle comporte en outre :

10 - des moyens pour découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i ,

- des moyens pour chiffrer le contenu du
15 flux à chaque changement de crypto-période i au moyen de la clé CW_i ,

- des moyens pour calculer un message de contrôle de titre d'accès $SC-ECM_i$ en fonction des clés CW_{i-1} , CW_i , CW_{i+1} correspondant respectivement aux
20 crypto-périodes CP_i , CP_{i-1} et CP_{i+1} , d'un paramètre de parité $p(i)$ et du critère de contrôle d'accès CA_i , le message $SC-ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

25 - des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s ,

- des moyens pour chiffrer les mots de contrôle CW_{i-1} , CW_i , CW_{i+1} au moyen d'une clé de
30 relecture KP_c ,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c .

5 21. Récepteur de désembrouillage (4) d'un flux de données diffusé sous forme embrouillée par une clé d'embrouillage CW_i comportant un processeur de sécurité comprenant au moins une clé KR_c destinée à désembrouiller des messages R- ECM_c de contrôle d'accès
10 à l'enregistrement et au moins une clé KP_c destinée à désembrouiller des messages P- ECM_c de contrôle d'accès à la relecture, récepteur caractérisé en ce qu'il comporte :

15 - des moyens pour récupérer la voie ECM des messages P- ECM_c et des messages R- ECM_c à partir de la signalisation rattachée au service diffusant le contenu ;

20 - des moyens pour déchiffrer les messages R- ECM_c au moyen de la clé d'enregistrement KR_c pour vérifier le droit à enregistrer le contenu d'un flux reçu,

25 - des moyens pour déchiffrer les messages P- ECM_c au moyen de la clé KP_c pour vérifier le droit à relire le contenu d'un flux enregistré.

30 22. Récepteur selon la revendication 21, caractérisé en ce qu'il comporte en outre des moyens pour générer une clé locale K_l à partir d'attributs contenus dans le message R- ECM_c de l'identité du récepteur pour chiffrer et déchiffrer localement le contenu du flux reçu.

23. récepteur selon la revendication 21, caractérisé en ce que le processeur de sécurité est une carte à puce.

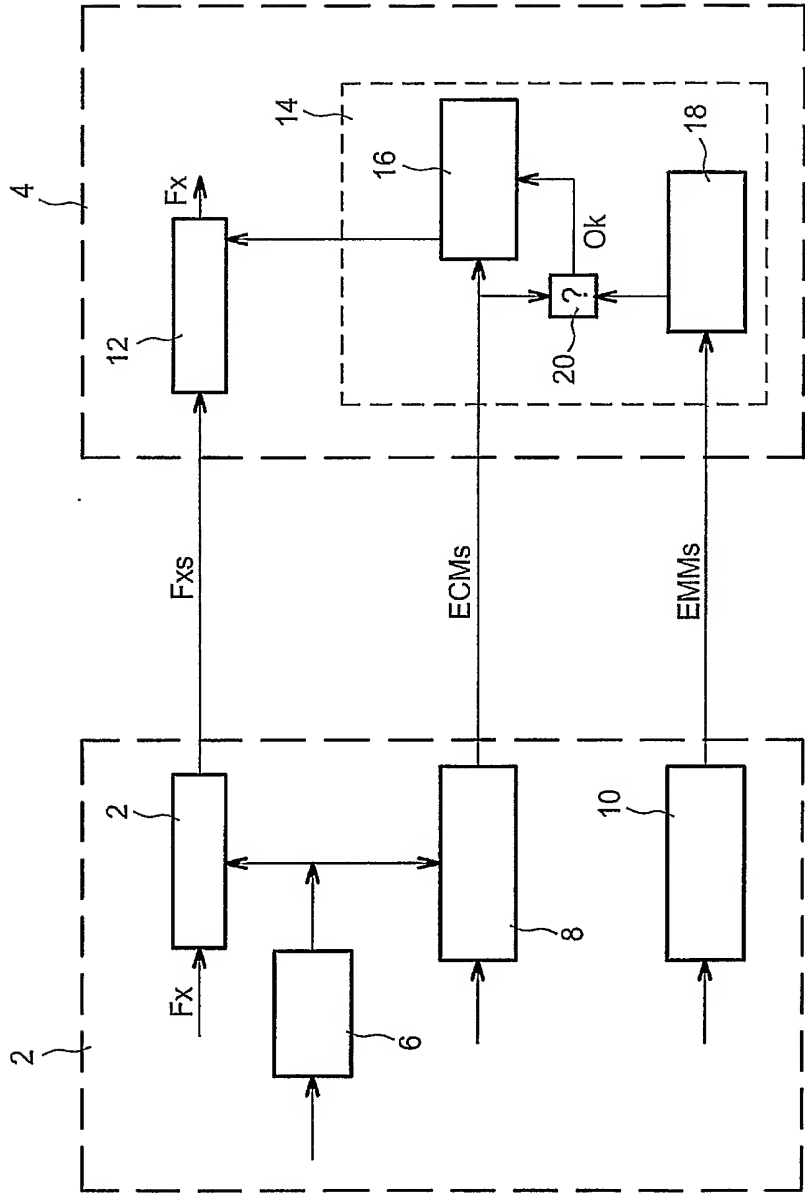


FIG. 1

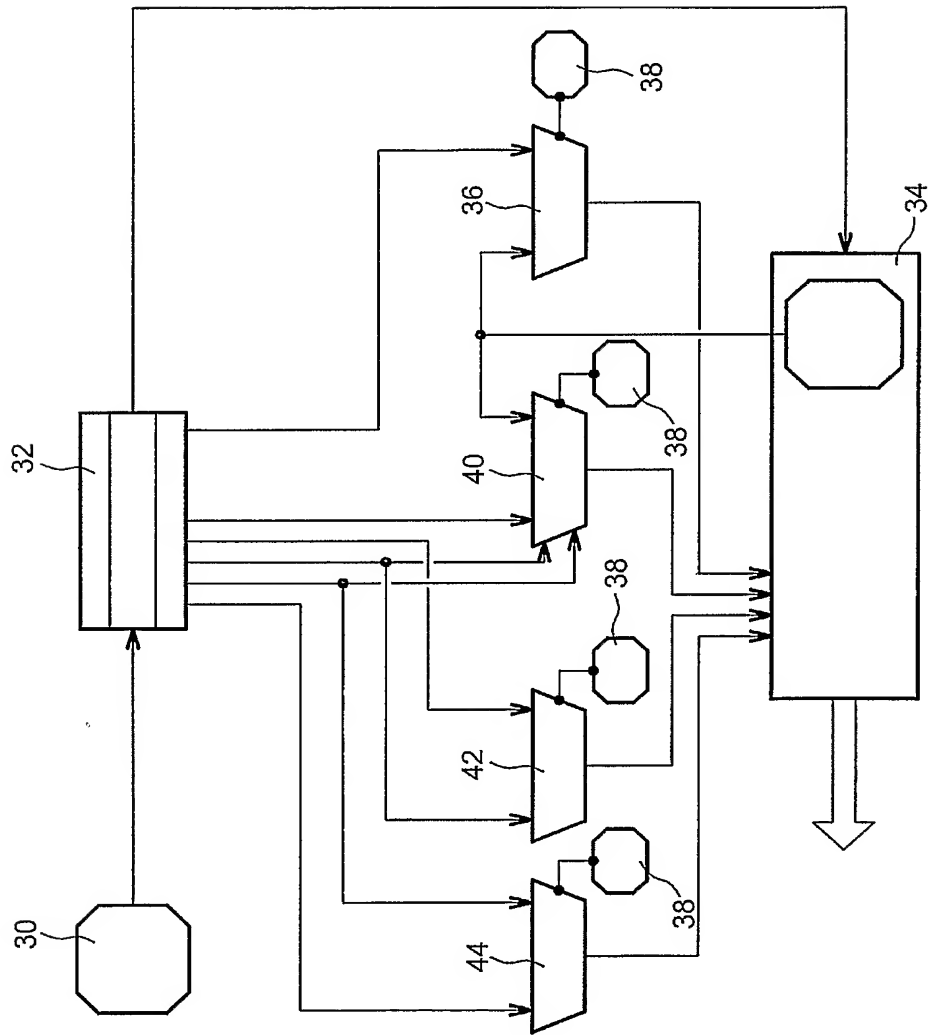


FIG. 2

3 / 4

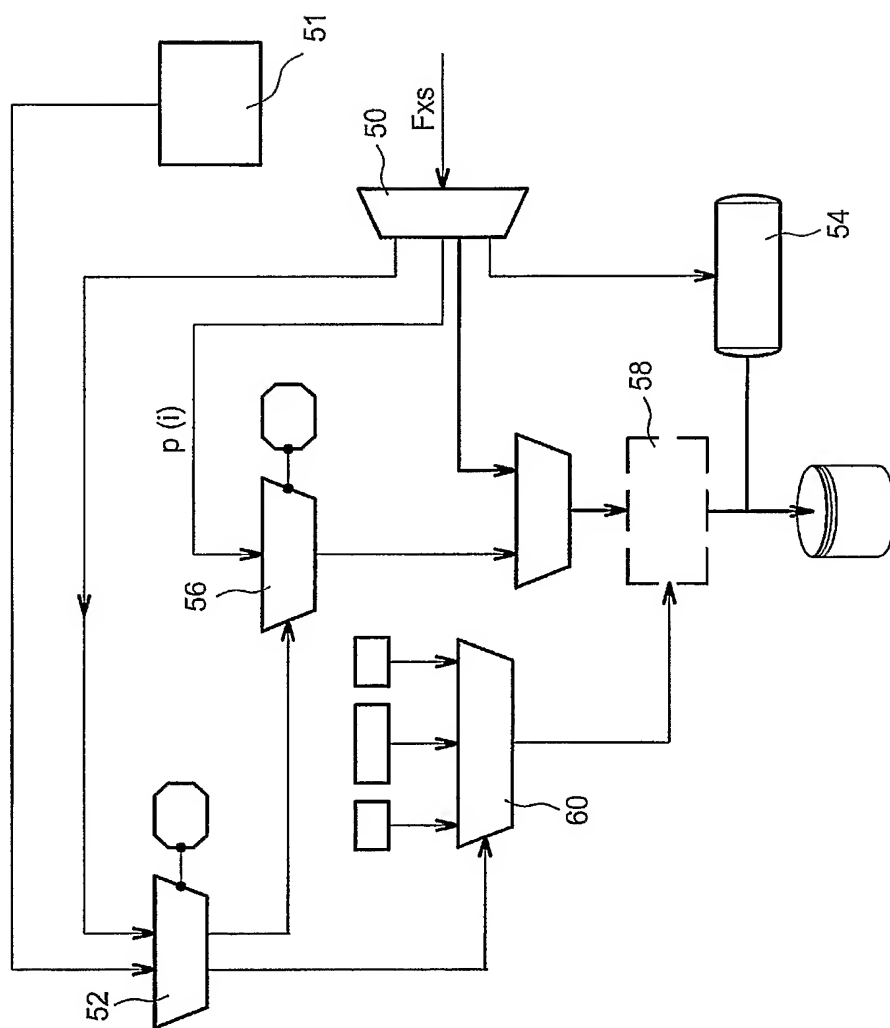


FIG. 3

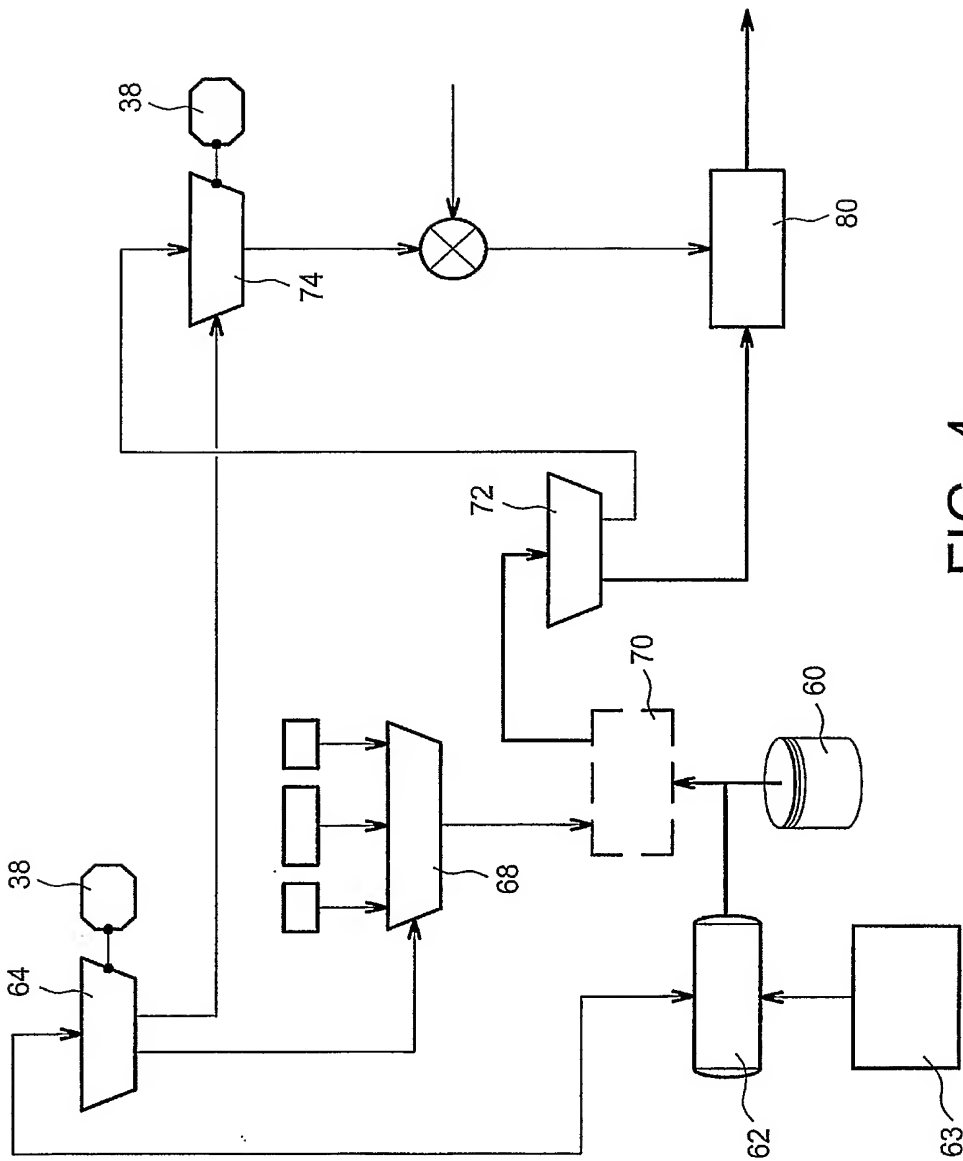


FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 03/50207

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04L9/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 936 774 A (CANAL PLUS SA) 18 August 1999 (1999-08-18) paragraphs '0038!, '0039! paragraphs '0060!, '0062!, '0063! paragraphs '0068! - '0071! -----	1,15,16, 18,21
Y	EP 0 691 787 A (SONY CORP) 10 January 1996 (1996-01-10) column 1, line 1 - line 24 column 17, line 11 - line 34 figures 6,7A,7B -----	1,15,16, 18,21
A	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) column 3, line 2 - line 11 column 3, line 32 - line 54 ----- -/--	1-23

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

G document member of the same patent family

Date of the actual completion of the international search

14 December 2004

Date of mailing of the international search report

21/12/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Tito Martins, J

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 03/50207

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 2001/014974 A1 (YOSHIDA SUNAO ET AL) 16 August 2001 (2001-08-16) paragraphs '0029!, '0030! -----</p>	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 03/50207

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0936774	A	18-08-1999	EP 0936774 A1	18-08-1999
			AT 225999 T	15-10-2002
			AT 258349 T	15-02-2004
			AU 754015 B2	31-10-2002
			AU 2295199 A	30-08-1999
			AU 749013 B2	13-06-2002
			AU 2296499 A	30-08-1999
			BR 9907877 A	31-10-2000
			BR 9907878 A	31-10-2000
			CA 2318879 A1	19-08-1999
			CA 2318992 A1	19-08-1999
			CN 1305674 T	25-07-2001
			CN 1296695 T	23-05-2001
			DE 69903408 D1	14-11-2002
			DE 69903408 T2	18-06-2003
			DE 69914306 D1	26-02-2004
			DE 69914306 T2	25-11-2004
			EP 0936812 A1	18-08-1999
			EP 1057332 A1	06-12-2000
			EP 1055305 A1	29-11-2000
			ES 2185311 T3	16-04-2003
			ES 2214840 T3	16-09-2004
			HK 1031070 A1	11-07-2003
			HR 20000486 A1	28-02-2001
			HR 20000487 A1	28-02-2001
			HU 0100651 A2	28-06-2001
			HU 0101456 A2	28-09-2001
			WO 9941907 A1	19-08-1999
			WO 9941874 A1	19-08-1999
			ID 26101 A	23-11-2000
			ID 25466 A	05-10-2000
			JP 2002503919 T	05-02-2002
			JP 2002514834 T	21-05-2002
			NO 20004062 A	13-10-2000
			NO 20004063 A	13-10-2000
			PL 342260 A1	04-06-2001
			PL 342261 A1	04-06-2001
			RU 2225681 C2	10-03-2004
			TR 200002348 T2	21-12-2000
			TR 200002350 T2	22-01-2001
			US 6714650 B1	30-03-2004
			ZA 9901122 A	30-09-1999
			ZA 9901123 A	12-08-1999
EP 0691787	A	10-01-1996	CN 1390043 A	08-01-2003
			CN 1390042 A	08-01-2003
			CN 1390054 A	08-01-2003
			CN 1390055 A	08-01-2003
			CN 1390056 A	08-01-2003
			CN 1390052 A	08-01-2003
			CN 1389993 A	08-01-2003
			CN 1390053 A	08-01-2003
			CN 1115150 A , B	17-01-1996
			DE 69523220 D1	22-11-2001
			DE 69523220 T2	13-06-2002
			DE 69530622 D1	05-06-2003
			DE 69530622 T2	26-02-2004
			EP 1126705 A2	22-08-2001

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 03/50207

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0691787 A		EP 1244306 A2	25-09-2002
		EP 0691787 A1	10-01-1996
		EP 0975165 A2	26-01-2000
		JP 8077706 A	22-03-1996
		JP 2003134104 A	09-05-2003
		JP 2003163659 A	06-06-2003
		JP 2003143547 A	16-05-2003
		JP 2003101942 A	04-04-2003
		JP 2003116120 A	18-04-2003
		JP 2003116101 A	18-04-2003
		JP 2003143548 A	16-05-2003
		JP 2003177970 A	27-06-2003
		JP 2004152481 A	27-05-2004
		JP 2004166286 A	10-06-2004
		US 5796828 A	18-08-1998
		US RE38007 E1	25-02-2003
EP 0858184 A	12-08-1998	IL 120174 A	28-10-1999
		EP 0858184 A2	12-08-1998
		US 6178242 B1	23-01-2001
		GB 2322030 A , B	12-08-1998
US 2001014974 A1	16-08-2001	JP 2001223953 A	17-08-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 03/50207

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167 H04L9/14

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04N H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 936 774 A (CANAL PLUS SA) 18 août 1999 (1999-08-18) alinéas '0038!, '0039! alinéas '0060!, '0062!, '0063! alinéas '0068! - '0071!	1,15,16, 18,21
Y	EP 0 691 787 A (SONY CORP) 10 janvier 1996 (1996-01-10) colonne 1, ligne 1 - ligne 24 colonne 17, ligne 11 - ligne 34 figures 6,7A,7B	1,15,16, 18,21
A	EP 0 858 184 A (NDS LTD) 12 août 1998 (1998-08-12) colonne 3, ligne 2 - ligne 11 colonne 3, ligne 32 - ligne 54	1-23
	-/--	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *Z* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

14 décembre 2004

Date d'expédition du présent rapport de recherche internationale

21/12/2004

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Tito Martins, J

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 03/50207

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>US 2001/014974 A1 (YOSHIDA SUNAO ET AL)</p> <p>16 août 2001 (2001-08-16)</p> <p>alinéas '0029!, '0030!</p> <p>-----</p>	1-23

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No

PCT/FR 03/50207

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0936774	A	18-08-1999	EP 0936774 A1	18-08-1999
			AT 225999 T	15-10-2002
			AT 258349 T	15-02-2004
			AU 754015 B2	31-10-2002
			AU 2295199 A	30-08-1999
			AU 749013 B2	13-06-2002
			AU 2296499 A	30-08-1999
			BR 9907877 A	31-10-2000
			BR 9907878 A	31-10-2000
			CA 2318879 A1	19-08-1999
			CA 2318992 A1	19-08-1999
			CN 1305674 T	25-07-2001
			CN 1296695 T	23-05-2001
			DE 69903408 D1	14-11-2002
			DE 69903408 T2	18-06-2003
			DE 69914306 D1	26-02-2004
			DE 69914306 T2	25-11-2004
			EP 0936812 A1	18-08-1999
			EP 1057332 A1	06-12-2000
			EP 1055305 A1	29-11-2000
			ES 2185311 T3	16-04-2003
			ES 2214840 T3	16-09-2004
			HK 1031070 A1	11-07-2003
			HR 20000486 A1	28-02-2001
			HR 20000487 A1	28-02-2001
			HU 0100651 A2	28-06-2001
			HU 0101456 A2	28-09-2001
			WO 9941907 A1	19-08-1999
			WO 9941874 A1	19-08-1999
			ID 26101 A	23-11-2000
			ID 25466 A	05-10-2000
			JP 2002503919 T	05-02-2002
			JP 2002514834 T	21-05-2002
			NO 20004062 A	13-10-2000
			NO 20004063 A	13-10-2000
			PL 342260 A1	04-06-2001
			PL 342261 A1	04-06-2001
			RU 2225681 C2	10-03-2004
			TR 200002348 T2	21-12-2000
			TR 200002350 T2	22-01-2001
			US 6714650 B1	30-03-2004
			ZA 9901122 A	30-09-1999
			ZA 9901123 A	12-08-1999
EP 0691787	A	10-01-1996	CN 1390043 A	08-01-2003
			CN 1390042 A	08-01-2003
			CN 1390054 A	08-01-2003
			CN 1390055 A	08-01-2003
			CN 1390056 A	08-01-2003
			CN 1390052 A	08-01-2003
			CN 1389993 A	08-01-2003
			CN 1390053 A	08-01-2003
			CN 1115150 A , B	17-01-1996
			DE 69523220 D1	22-11-2001
			DE 69523220 T2	13-06-2002
			DE 69530622 D1	05-06-2003
			DE 69530622 T2	26-02-2004
			EP 1126705 A2	22-08-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs àmembres de familles de brevets

Demande Internationale No

PCT/FR 03/50207

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0691787 A		EP 1244 306 A2	25-09-2002
		EP 0691 787 A1	10-01-1996
		EP 0975 165 A2	26-01-2000
		JP 8077 706 A	22-03-1996
		JP 2003134 104 A	09-05-2003
		JP 2003163 659 A	06-06-2003
		JP 2003143 547 A	16-05-2003
		JP 2003101 942 A	04-04-2003
		JP 2003116 120 A	18-04-2003
		JP 2003116 101 A	18-04-2003
		JP 2003143 548 A	16-05-2003
		JP 2003177 970 A	27-06-2003
		JP 2004152 481 A	27-05-2004
		JP 2004166 286 A	10-06-2004
		US 5796 828 A	18-08-1998
		US RE38 007 E1	25-02-2003
EP 0858184 A	12-08-1998	IL 120 174 A	28-10-1999
		EP 0858 184 A2	12-08-1998
		US 6178 242 B1	23-01-2001
		GB 2322 030 A , B	12-08-1998
US 2001014974 A1	16-08-2001	JP 2001223953 A	17-08-2001